

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-105472

(43) 公開日 平成10年(1998) 4月24日

(51) Int.Cl.⁹

G 0 6 F 12/14

G 0 6 K 17/00
19/073

識別記号

3 2 0

3 1 0

F I

G 0 6 F 12/14

G 0 6 K 17/00
19/00

3 2 0 C

3 1 0 K

D

P

審査請求 未請求 請求項の数14 F D (全 16 頁)

(21) 出願番号

特願平8-278877

(22) 出願日

平成8年(1996) 9月30日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 飯島 康雄

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

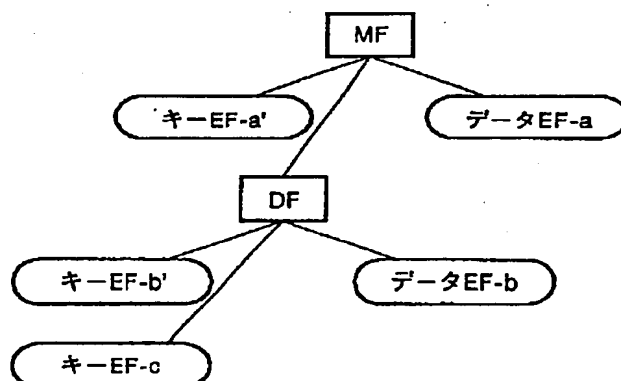
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 メモリのアクセス管理方法

(57) 【要約】

【課題】上位者からのデータファイルへの関与をなくし、上位者から下位者へ当該データファイルまたはメモリ領域へのアクセスの権限を委譲する。

【解決手段】メモリを複数のファイルに分割してなるICカードにおいて、下位者は、上位者が設定したトランSPORTキーを自身のみが知りえるキー(b')に当該キーEFに設定されているキー変更用のアクセス条件を参照して変更し、データファイル(DF)に付与されているトランSPORTビットをオンにし、自身が必要とするデータEF-bをデータファイル(DF)に設定されているEF創成用アクセス条件を参照してデータファイル(DF)配下に創成し、自身が必要とするキーEF-cをデータファイル(DF)に設定されているEF創成用アクセス条件を参照してデータファイル(DF)配下に創成する。



【特許請求の範囲】

【請求項1】 メモリを複数のファイルに分割し、この分割した複数のファイルに対してのアクセスをそれぞれ管理するもので、当該メモリを用いたシステムの上位者にてファイル配下に第1のキーが予め設定されており、当該メモリを用いたシステムの下位者が新たにキーを設定可能に構成されており、かつ、これらのキーの照合によって上記ファイルへのアクセスを可能とするメモリのアクセス管理方法であって、

上記上位者が設定した第1のキーを、この第1のキーに設定されているキー変更用のアクセス条件を参照して下位者のみが知りえる第2のキーに変更し、この第2のキーに変更された際、上記上位者によるファイル配下のキー創成を拒絶するようにしたことを特徴とするメモリのアクセス管理方法。

【請求項2】 メモリを複数のファイルに分割し、この分割した複数のファイルに対してのアクセスをそれぞれ管理するもので、当該メモリを用いたシステムの上位者にてファイル配下に第1のキーが予め設定されており、当該メモリを用いたシステムの下位者が新たにキーを設定可能に構成されており、かつ、これらのキーの照合によって上記ファイルへのアクセスを可能とするメモリのアクセス管理方法であって、

上記上位者が設定した第1のキーを、この第1のキーに設定されているキー変更用のアクセス条件を参照して下位者のみが知りえる第2のキーに変更し、上記上位者によるファイル配下のキー創成を拒絶するようにしたことを特徴とするメモリのアクセス管理方法。

【請求項3】 上位のファイルと下位のファイルとからなるツリー構造のファイルへのアクセスを管理するファイルアクセス管理方法において、

上位の管理者が管理する上位のファイルに対してアクセス条件を設定し、

上位の管理者から下位の管理者に対して提供するファイルにアクセス条件を設定し、

上位の管理者から下位の管理者に対する受け渡しのためのトランスポートキーを下位のファイルに設定する場合は、当該ファイルの上位のファイルのアクセス条件を参照し、

この上位のファイルのアクセス条件を満足している場合にトランスポートキーを下位のファイルに設定し、

下位のファイルの配下にファイルを設定する場合は当該下位ファイルのアクセス条件を参照してこのアクセス条件を満足している場合にファイルの設定を行うようにしたことを特徴とするファイルアクセス管理方法。

【請求項4】 前記下位のファイルにはトランスポートキーの設定の可否を示す識別情報が付与されており、この識別情報に基づき該ファイルに対するトランスポートキーの設定を禁止するようにしたことを特徴とする請求項3に記載のファイルアクセス管理方法。

【請求項5】 前記下位のファイルに対するトランスポートキーが変更された場合、以後該ファイルに対するトランスポートキーの設定を禁止するように前記識別情報を更新するようにしたことを特徴とする請求項4に記載のファイルアクセス管理方法。

【請求項6】 前記下位のファイルにおけるトランスポートキーの設定の可否を示す識別情報は特殊コマンドに基づき更新するようにしたことを特徴とする請求項4に記載のファイルアクセス管理方法。

10 【請求項7】 前記下位のファイルへのトランスポートキーの設定はトランスポートキー設定用のコマンドにより行い、前記下位のファイルの配下にファイルを設定する場合はトランスポートキー設定用のコマンドとは異なるコマンドにより行うことを特徴とする請求項3に記載のファイルアクセス管理方法。

【請求項8】 上位のファイルと下位のファイルとからなるツリー構造のファイルを有する携帯可能情報処理装置において、

20 アクセス条件が設定され上位の管理者が利用するための上位のファイルと、

アクセス条件が設定され上位の管理者から提供され下位の管理者が利用する下位のファイルと、

上位のファイルのアクセス条件を参照してこの上位のファイルのアクセス条件を満足している場合に上位の管理者から下位の管理者に対する受け渡しのためのトランスポートキーを下位のファイルに設定する第1の手段と、下位ファイルのアクセス条件を参照してこのアクセス条件を満足している場合に下位のファイルの配下にファイルを設定する第2の手段と、

30 を有することを特徴とする携帯可能情報処理装置。

【請求項9】 前記下位のファイルにはトランスポートキーの設定の可否を示す識別情報の記憶領域を有し、この識別情報に基づき該ファイルに対するトランスポートキーの設定を禁止する手段を有することを特徴とする請求項8に記載の携帯可能情報処理装置。

40 【請求項10】 前記下位のファイルに対するトランスポートキーが変更された場合、以後該ファイルに対するトランスポートキーの設定を禁止するように前記識別情報を更新する手段を有することを特徴とする請求項8に記載の携帯可能情報処理装置。

【請求項11】 前記携帯可能情報記憶媒体は、外部装置から供給されるコマンドに基づき動作し、前記下位のファイルにおけるトランスポートキーの設定の可否を示す識別情報は外部装置より供給される特殊コマンドに基づき更新する手段を有することを特徴とする請求項8に記載の携帯可能情報処理装置。

50 【請求項12】 前記携帯可能情報記憶媒体は、外部装置から供給されるコマンドに基づき動作し、前記第1の手段による下位のファイルへのトランスポートキーの設定はトランスポートキー設定用のコマンドに

より動作し、前記第2の手段による下位のファイルの配下へのファイルの設定はトランスポートキー設定用のコマンドとは異なるコマンドにより動作することを特徴とする請求項8に記載の携帯可能情報処理装置。

【請求項13】 上位のファイルと下位のファイルとからなるツリー構造のファイルを創成し、かつ制御手段により各ファイルへのアクセス管理を行う情報処理装置用制御プログラムを記憶した媒体において、

前記制御プログラムは前記制御手段に対して、

上位の管理者によりアクセス条件が設定された上位のファイルを作成させるステップと、

上位の管理者から提供され下位の管理者が利用するためにアクセス条件が設定され下位のファイルを作成させるステップと、

上位のファイルのアクセス条件を参照してこの上位のファイルのアクセス条件を満足している場合に上位の管理者から下位の管理者に対する受け渡しのためのトランスポートキーを下位のファイルに設定させるステップと、下位ファイルのアクセス条件を参照してこのアクセス条件を満足している場合に下位のファイルの配下にファイルを設定させるステップとから構成されこの制御プログラムを記憶したことを特徴とする情報処理装置用制御プログラムを記憶した媒体。

【請求項14】 前記情報処理装置用制御プログラムを記憶したプログラムメモリと、前記ファイルが割り当てられるデータメモリと、該ファイルへのアクセス管理を行う制御回路と、外部装置とのインターフェイスが1つのモジュール内に構成されていることを特徴とする請求項13に記載の情報処理装置用制御プログラムを記憶した媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、たとえば、不揮発性メモリ、および、これらを制御するCPUなどの制御素子を有するICチップを内蔵したICカードなどの電子装置において、上記メモリ内に分割設定される複数のファイルに対してのアクセスを管理するメモリのアクセス管理方法に関する。

【0002】

【従来の技術】 最近、携帯可能なデータ記憶媒体として、不揮発性のデータメモリ、および、これらを制御するCPU（セントラル・プロセッシング・ユニット）などの制御素子を有するICチップを内蔵したICカードが注目されている。

【0003】 この種のICカードは、内蔵するデータメモリを複数のファイルに分割し、かつ、個々のファイルには、利用アプリケーションが運用時に必要なデータなどが格納されるようになっており、外部装置からアプリケーション識別名などを入力することにより、選択的に対応ファイルのみが使用可能な状態を実現するようにな

っている。このため、複数のアプリケーションデータをファイル分けし、1枚のICカードに格納することにより、多目的利用が可能となっている。

【0004】 さて、この多目的を指向するICカードにおいては、カード発行者及びアプリケーション提供者の権限を明確に区分する事が要求される。

【0005】 この権限とは、各当事者に割り当てられている暗証番号が照合された際、ICカードへのアクセスの可否範囲を明確にする事で実現できる。

10 【0006】 従来のICカードでは、カード発行者がアプリケーション提供者に対してファイルを提供する際、当該ファイルにアプリケーション提供者に対するトランスポートキーを設定する。アプリケーション提供者は、このカードを受け取ると、まず当該トランスポートキーを自身のみが知りえる提供者キーに書き換え、この後、アプリケーション提供者に与えられたファイル内の管理を、この提供者キーにて行えるようになされている。

20 【0007】 さてここで、ファイル内の管理を行える環境を定義する情報として、一般的に、当該ファイルに付与されたアクセス条件が挙げられる。つまり、カード発行者がアプリケーション提供者に提供するファイルには、アプリケーション提供者キーの照合が必要というアクセス条件が付与されるべきである。

【0008】 上述したファイル内の管理行為の一つとして、アプリケーションにて使用するファイルを設定することが挙げられる。この行為には、先に述べたアプリケーション提供者用トランスポートキーの設定をも含まれていることを考える。

30 【0009】 この場合、ファイル内の管理をアプリケーション提供者のみにて行わせるように当該ファイルのアクセス条件を設定すると、発行者がアプリケーション提供者用トランスポートキーを設定するために満足しなければならないアプリケーション提供者キーが存在していないため、発行者は、当該トランスポートキーを永久に設定できない事になる。

【0010】 これを回避するために、当該ファイルに与えるアクセス条件として、アプリケーション提供者キーまたは発行者キーのいずれかと設定する方法が考えられる。

40 【0011】 つまり、発行者が当該ファイルにアプリケーション提供者用トランスポートキーを設定する場合、発行者キーを照合することによりアクセス条件を満足させ、一方、アプリケーション提供者が当該ファイル内の他の管理行為を行う場合には、自身のアプリケーション提供者キーを照合することによりアクセス条件を満足させるようにアクセス条件を設定すれば良い。

50 【0012】 しかしながら、この場合、当該ファイルに設定されているアクセス条件は発行者とアプリケーション提供者の双方によりアクセス可能となり、当該ファイルへの管理権限は、発行者（上位者）からアプリケーシ

ョン提供者（下位者）に委譲されたとは言えないことになる。

【0013】

【発明が解決しようとする課題】上記したように、発行者が当該ファイルにアプリケーション提供者用トランスポートキーを設定する場合、発行者キーを照合することによりアクセス条件を満足させ、一方、アプリケーション提供者が当該ファイル内の他の管理行為を行う場合には、自身のアプリケーション提供者キーを照合することによりアクセス条件を満足させた場合、当該ファイルに設定されているアクセス条件により、当該ファイルへの管理権限は、発行者（上位者）からアプリケーション提供者（下位者）に委譲されたとは言えないという問題があった。

【0014】そこで、この発明は、たとえば、上位者からのデータファイルへの関与をなくし、上位者から下位者へ当該データファイルまたはメモリ領域へのアクセスの権限を委譲することができるメモリのアクセス管理方法を提供することを目的とする。

【0015】

【課題を解決するための手段】本発明のメモリのアクセス管理方法は、メモリを複数のファイルに分割し、この分割した複数のファイルに対してのアクセスをそれぞれ管理するもので、当該メモリを用いたシステムの上位者にてファイル配下に第1のキーが予め設定されており、当該メモリを用いたシステムの下位者が新たにキーを設定可能に構成されており、かつ、これらのキーの照合によって上記ファイルへのアクセスを可能とするメモリのアクセス管理方法であって、上記上位者が設定した第1のキーを、この第1のキーに設定されているキー変更用のアクセス条件を参照して下位者のみが知りえる第2のキーに変更し、この第2のキーに変更された際、上記上位者によるファイル配下のキー創成を拒絶するようにしたことを特徴とする。

【0016】本発明のメモリのアクセス管理方法は、メモリを複数のファイルに分割し、この分割した複数のファイルに対してのアクセスをそれぞれ管理するもので、当該メモリを用いたシステムの上位者にてファイル配下に第1のキーが予め設定されており、当該メモリを用いたシステムの下位者が新たにキーを設定可能に構成されており、かつ、これらのキーの照合によって上記ファイルへのアクセスを可能とするメモリのアクセス管理方法であって、上記上位者が設定した第1のキーを、この第1のキーに設定されているキー変更用のアクセス条件を参照して下位者のみが知りえる第2のキーに変更し、上記上位者によるファイル配下のキー創成を拒絶するようにしたことを特徴とする。

【0017】本発明のファイルアクセス管理方法は、上位のファイルと下位のファイルとからなるツリー構造のファイルへのアクセスを管理するファイルアクセス管理

方法において、上位の管理者が管理する上位のファイルに対してアクセス条件を設定し、上位の管理者から下位の管理者に対して提供するファイルにアクセス条件を設定し、上位の管理者から下位の管理者に対する受け渡しのためのトランスポートキーを下位のファイルに設定する場合は、当該ファイルの上位のファイルのアクセス条件を参照し、この上位のファイルのアクセス条件を満足している場合にトランスポートキーを下位のファイルに設定し、下位のファイルの配下にファイルを設定する場合は当該下位ファイルのアクセス条件を参照してこのアクセス条件を満足している場合にファイルの設定を行うようにしたことを特徴とする。

【0018】本発明の携帯可能情報処理装置は、上位のファイルと下位のファイルとからなるツリー構造のファイルを有する携帯可能情報処理装置において、アクセス条件が設定され上位の管理者が利用するための上位のファイルと、アクセス条件が設定され上位の管理者から提供され下位の管理者が利用する下位のファイルと、上位のファイルのアクセス条件を参照してこの上位のファイルのアクセス条件を満足している場合に上位の管理者から下位の管理者に対する受け渡しのためのトランスポートキーを下位のファイルに設定する第1の手段と、下位ファイルのアクセス条件を参照してこのアクセス条件を満足している場合に下位のファイルの配下にファイルを設定する第2の手段とから構成されている。

【0019】本発明の情報処理装置用制御プログラムを記憶した媒体は、上位のファイルと下位のファイルとからなるツリー構造のファイルを創成し、かつ制御手段により各ファイルへのアクセス管理を行う情報処理装置用制御プログラムを記憶した媒体において、前記制御プログラムは前記制御手段に対して、上位の管理者によりアクセス条件が設定された上位のファイルを創成させるステップと、上位の管理者から提供され下位の管理者が利用するためにアクセス条件が設定され下位のファイルを創成させるステップと、上位のファイルのアクセス条件を参照してこの上位のファイルのアクセス条件を満足している場合に上位の管理者から下位の管理者に対する受け渡しのためのトランスポートキーを下位のファイルに設定させるステップと、下位ファイルのアクセス条件を参照してこのアクセス条件を満足している場合に下位のファイルの配下にファイルを設定させるステップとから構成されこの制御プログラムを記憶したことを特徴とする。

【0020】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【0021】図1は、本実施の形態に係る携帯可能電子装置としてのICカードが適用される、たとえば、金融システムあるいはショッピングシステムなどの端末装置として用いられるカード取扱装置の構成例を示すもので

10

20

30

40

50

ある。すなわち、この装置は、ICカード1をカードリーダー・ライタ2を介してCPUなどからなる制御部3と接続可能とするとともに、制御部3にキーボード4、CRTディスプレイ装置5、プリンタ6、および、フロッピーディスク装置7を接続して構成される。

【0022】図2は、ICカード1の構成例を示すものであり、制御部としての制御素子（たとえば、CPU）11、記憶内容が消去可能な不揮発性のデータメモリ12、ワーキングメモリ13、プログラムメモリ14、および、カードリーダー・ライタ2との電氣的接触を得るためのコンタクト部15によって構成されている。これらのうち、破線内の部分（制御素子11、データメモリ12、ワーキングメモリ13、プログラムメモリ14）は1つのICチップ（あるいは複数）10で構成されて、さらに、実開平2-17381号にて知られるように、ICチップ10とコンタクト部15とが一体的にICモジュール化されて、ICカード本体内に埋設されている。

【0023】データメモリ12は、各種データの記憶に使用され、たとえば、EEPROMなどで構成されている。ワーキングメモリ13は、制御素子11が処理を行なう際の処理データを一時的に保持するためのメモリであり、たとえば、RAMなどで構成される。プログラムメモリ14は、たとえば、マスクROMで構成されており、制御素子11のプログラムなどを記憶するものである。

【0024】データメモリ12は、たとえば、図3に示すように、制御領域120、ディレクトリ121、空き領域122、および、エリア群123に分割されている。エリア群123は、複数のデータエリアおよびキーエリアを有することができ、かつ、データファイル（DF）と呼ばれる概念でグループ化することができる。なお、後述するマスタファイル（MF）は、データファイルの1つの形態として一括管理される。

【0025】データファイルは、対応するアプリケーションにて使用されるデータエリア、および、キーエリアを一括して管理するためのファイルである。

【0026】データエリアは、たとえば、取引データなどのように、必要に応じて読み書きするためのデータを格納するエリアである。

【0027】キーエリアは、たとえば、暗証番号などの格納に利用されているエリアであり、書込み／書換え／照合の対象になり、読出しはできないようになっている。

【0028】なお、これらのエリアは、図3に示すように、エリア群123として一括して割当てられている。また、これらのファイルあるいはエリアは、データメモリ12内のディレクトリ121を用いることにより、それぞれの物理的位置などを制御素子11が認識するようになっている。

【0029】さらに、図3の制御領域120には、エリア群123の先頭アドレス情報、および、空き領域122の先頭アドレス情報が格納されている。

【0030】図3のディレクトリ121は、図4に示すように、各データファイルおよびエリアに対応する各種定義情報が格納される。

【0031】図4（a）は、データファイルの名称を定義する情報である。この定義情報は、ディレクトリ121内でデータファイル名定義情報を識別するためのデータPTN、本データファイルに割当てられたファイル通し番号DFSN、本データファイルの親ファイルの通し番号PFSN、本データファイルに付与されたファイル名DFnameおよびその長さを示すデータNL、および、これらのデータの正当性をチェックするためのデータBCCから構成される。

【0032】図4（b）は、データファイルの管理情報を定義する情報である。この定義情報は、ディレクトリ121内でデータファイル名定義情報を識別するためのデータPTN、本データファイルに割当てられたファイル通し番号DFSN、本データファイルの親ファイルの通し番号PFSN、データファイルサイズDFS、本データファイルの付加情報が格納されるデータエリアを識別するためのAAID、当該付加情報を出力するか否かなどを規定するTYPE、キーの種別を禁止するUCF、データファイルのアクセス条件を示すDFAC、本データファイルの状態を保持するためのDFST、本データファイルの配下に位置するデータファイルおよびエリアにより使用されているバイト数US、および、これらのデータの正当性をチェックするためのデータBCCから構成される。

【0033】ここでDFSTの特定ビット（例えば8ビット目）は、該DFのトランスポートキーが変更されたか否かを示すトランスポートビットとして使用される。

【0034】また、特にAAIDは、後述するデータファイル選択コマンドにてデータファイルが選択された際に、必要に応じてそれに示されるデータエリアの内容を出力する。

【0035】図4（c）は、各種取引データなどを格納するエリアを定義する情報である。この定義情報は、ディレクトリ121内でエリア定義情報を識別するためのデータPTN、本エリアが属するデータファイルの通し番号DFSN、エリアに対してアクセスする際の識別番号AID、エリアの先頭アドレスを示すATOP、エリアサイズを示すASIZ、エリアのアクセス条件を示すAAC、エリアの状態を保持するAST、および、これらのデータの正当性をチェックするためのデータBCCから構成される。

【0036】図4（d）は、各種キーデータを格納するエリアを定義する情報である。この定義情報は、ディレクトリ121内でキーエリア定義情報を識別するための

データPTN、本エリアが属するデータファイルの通し番号DFSN、エリアに対してアクセスする際の識別番号KID、エリアの先頭アドレスを示すKTOP、エリアサイズを示すKSIZ、キーの種別を示すCF、キーのアクセス条件を示すKAC、キーの状態を保持するKST、および、これらのデータの正当性をチェックするためのデータBCCから構成される。

【0037】これらに使用されている識別情報PTNは、たとえば、1バイトで構成されており、データファイルの名称を定義するもの(図4(a))に対しては'00'が、データファイルの管理情報を定義するもの(図4(b))に対しては'01'が、データエリアを定義するもの(図中(c))に対しては'02'が、また、キーエリアを定義するもの(図4(d))に対しては'03'が、それぞれ使用される。

【0038】図5は、ファイルの構造例を示している。この図において、DFnnはデータファイルを、Dnnはデータエリアを、Knnはキーエリアを、それぞれ示している。

【0039】図示するように、ICカード1内のメモリ12において、マスタファイル(MF)の配下には、データファイルDF1、DF2が、また、キーエリアK00、K01、データエリアD00、D01が、それぞれ設定されている。

【0040】また、データファイルDF1の配下には、データファイルDF1-1、DF1-2が、また、キーエリアK11、K12、データエリアD11、D12が、それぞれ設定されている。

【0041】また、データファイルDF1-1の配下には、キーエリアK111、K112、データエリアD111/D112が、また、データファイルDF1-2の配下には、キーエリアK121、K122、データエリアD121、D122が、それぞれ設定されている。

【0042】一方、データファイルDF2の配下には、データファイルDF2-1、DF2-2が、また、キーエリアK21、K22、データエリアD21、D22が、それぞれ設定されている。

【0043】また、データファイルDF2-1の配下には、キーエリアK211、K212、データエリアD211、D212が、また、データファイルDF2-2の配下には、キーエリアK221、K222、データエリアD221、D222が、それぞれ設定されている。

【0044】これらの各種定義情報は、一括して図6に示すように、ディレクトリ121に格納される。図示するように、各定義情報には、DFSN(ファイル通し番号)が、ファイル作成時に自動的に付与される。このDFSN、および、データファイル定義情報に格納される親ファイルのシーケンス番号により、各ファイルの関連状態を制御素子11が認識する。

【0045】たとえば、データファイルDF1-1の定

義情報(通し番号#13)は、DFSNが'03'、また、PFSNが'01'となっている。すなわち、本データファイルは、ファイルシーケンス番号'03'が作成時に付与され、同時に本データファイルがDF1の配下に作成されることを認識し、データファイルDF1のDFSN('01')をPFSNとして付与する。

【0046】図7は、データファイル(DF)作成のための動作を説明するフローチャートを示しており、以下それについて説明する。ICカード1が、外部から入力されるデータファイル作成コマンドを受信すると、まず、使用可能状態、すなわち、カレント状態となっているデータファイル(以後、カレントDFと称す)を認識する(ST1)。特に、ICカード1への電気的活性化の直後は、カレントDFはマスタファイル(MF)となる。

【0047】カレントDFを認識すると、次に、カレントDF定義情報中のアクセス条件情報のうち、ファイル作成に関する情報を参照する。この条件と、後述するRAM上の照合状態保持領域Aのみを比較し、アクセス条件が要求しているキーの照合状態が確立されているか否かを判断する(ST2)。

【0048】もし確立されていなければ、アクセス条件不一致を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST3)。また、もし確立されていれば、次に、コマンド内に設定されているデータファイルのファイル名(DF-ID)を抽出し、カレントDFが有するFSNと同一の値を親FSNとして有しており、さらに、抽出したファイル名と同一のファイル名を有しているデータファイル定義情報が存在するか否かを確認する(ST4)。

【0049】もし存在するとしたら、ID重複異常を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST5)。また、もし存在しないとしたら、コマンドにて与えられたデータファイル作成のためのデータにより、図4(a)~(c)に示すデータファイル定義情報を生成し(ST6)、これを所定領域に書込む(ST7)。

【0050】この書込みにおいて、書込みが正常に終了しなかった場合(ST8)、データ書込み異常を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST9)。また、書込みが正常に終了した場合(ST8)、正常終了を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST10)。

【0051】図8は、キーエレメンタリファイル(EF)作成のための動作を説明するフローチャートを示しており、以下それについて説明する。ICカード1が、外部から入力されるキー-EF作成コマンドを受信すると、まず、カレントDFを認識する(ST11)。

【0052】カレントDFを認識すると、次に、カレントDF定義情報中のアクセス条件情報のうち、ファイル

10

20

30

40

50

創成に関する情報を参照する。この条件と、後述するRAM上の照合状態保持領域Aのみを比較し、アクセス条件が要求しているキーの照合状態が確立されているか否かを判断する(ST12)。

【0053】もし確立されていなければ、アクセス条件不一致を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST13)。また、もし確立されていれば、次に、コマンド電文にて指示されているエレメンタリファイル名(EF-ID)を参照し、アクセス対象となっているカレントDF内に、当該エレメンタリファイル名が存在するか否かをチェックする(ST14)。もし存在する場合には、ID重複異常を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST15)。

【0054】もし存在しなければ、次に、コマンド電文にて指定されているキーEFのサイズデータを参照し、アクセス対象となっているカレントDF内の空き領域サイズと比較する(ST16)。この比較においては、指定されたキーEFのサイズに当該キーEFを創成した際に使用するディレクトリ情報のサイズを加算したものに
10 対して、前記空き領域サイズがそれ以上であるか否かを
チェックする。もし前者が後者よりも大きい場合には、
指定サイズ異常を示すレスポンス電文を出力し、コマ
ンド待ち状態に戻る(ST17)。

【0055】もしそうでなければ、次に、コマンド電文にて指定されたキーのタイプと、サイズの正当性をチェックする(ST18)。このとき、キーのタイプが「認証関連キー」となっていればサイズが例えば10バイト、また、キーのタイプが「照合キー」となっていればサイズは例えば3~18バイトであるとき、サイズが正
20 当であると判断する。もし正当でないと判断された場合
には、指定サイズ整合異常を示すレスポンス電文を出力
し、コマンド待ち状態に戻る(ST19)。

【0056】ここで、サイズが正当であったと判断された場合には、受信したコマンドに基づき、ディレクトリに格納すべきキーEF定義情報を生成し(ST20)、これを所定領域に書込む(ST21)。このとき、ステータス情報の第8ビット目は、コマンド電文にて指定されたキータイプ情報のうちの第1ビット目に依存して、その値が決定される。すなわち、後者のビット値と同様の値を前者のビットに設定する。

【0057】このステータス情報の第8ビット目は、キーデータの変更がなされたか否かを示すビットであり、当該ビットが「1」の場合、変更行為がなされていないことを示し、また、「0」であればその行為がなされたことを示している。

【0058】したがって、上記キータイプ情報の第1ビット目が「1」の場合には、キー変更を行なわない限りステータス情報の第8ビット目が「0」とはならず、また、「0」の場合には、キー変更を行なうか否かに関わらず、ステータス情報の第8ビット目が「0」となって

いる(つまり、書換え行為が暗黙的に行なわれたことと等価になる)。

【0059】上記キーEF定義情報の書込みにおいて、書込みが正常に終了しなかった場合(ST22)、データ書込み異常を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST23)。また、書込みが正常に終了した場合(ST22)、正常終了を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST24)。

【0060】図9は、トランスポートキーエレメンタリファイル(EF)を創成する場合の動作を説明するフローチャートを示しており、以下それについて説明する。ICカード1が、外部から入力されるトランスポートEF創成コマンドを受信すると、まず、カレントDFを認識する(ST101)。

【0061】カレントDFを認識すると、次に、当該データファイル(DF)に設定されているステータス情報DFST中のトランスポートビットがオンになっている
20 かどうかをチェックする(ST102)。

【0062】もしトランスポートビットがオンとなっていれば、当該コマンドは拒絶され、トランスポート不可を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST103)。また、もしトランスポートビットがオフとなっていれば、このトランスポートキーEF創成コマンドが許容される。なお、このトランスポートビットは、データファイル創成時にはオフとなっており、またトランスポートキー自身がキー変更コマンドにより変更された時点でオンとなる。

【0063】トランスポートキーEF創成コマンドが許容されると、次に、当該カレントDFの親データファイル(DF)のアクセス条件を参照する。この条件と、後述するRAM上の照合状態保持領域Aのみを比較し、アクセス条件が要求しているキーの照合状態が確立されているか否かを判断する(ST104)。

【0064】もし確立されていなければ、アクセス条件不一致を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST105)。また、もし確立されていれば、次に、コマンド電文にて指示されているエレメンタリファイル名(EF-ID)を参照し、アクセス対象となっているカレントDF内に、当該エレメンタリファイル名が存在するか否かをチェックする(ST106)。もし存在する場合には、ID重複異常を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST107)。

【0065】もし存在しなければ、次に、コマンド電文にて指定されているキーEFのサイズデータを参照し、アクセス対象となっているカレントDF内の空き領域サイズと比較する(ST108)。この比較においては、指定されたキーEFのサイズに当該キーEFを創成した際に使用するディレクトリ情報のサイズを加算したもの
50

に対して、前記空き領域サイズがそれ以上であるか否かをチェックする。もし前者が後者よりも大きい場合には、指定サイズ異常を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST109)。

【0066】もしそうでなければ、次に、コマンド電文にて指定されたキーのタイプと、サイズの正当性をチェックする(ST110)。このとき、キーのタイプが「認証関連キー」となっていればサイズが例えば10バイト、また、キーのタイプが「照合キー」となっていればサイズは例えば3~18バイトであるとき、サイズが正当であると判断する。もし正当でないと判断された場合には、指定サイズ整合異常を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST111)。

【0067】ここで、サイズが正当であったと判断された場合には、受信したコマンドに基づき、ディレクトリに格納すべきキーEF定義情報を生成し(ST112)、これを所定領域に書込む(ST113)。このとき、ステータス情報の第8ビット目は、コマンド電文にて指定されたキータイプ情報のうちの第1ビット目に依存して、その値が決定される。すなわち、後者のビット値と同様の値を前者のビットに設定する。

【0068】このステータス情報の第8ビット目は、キーデータの変更がなされたか否かを示すビットであり、当該ビットが「1」の場合、変更行為がなされていないことを示し、また、「0」であればその行為がなされたことを示している。

【0069】したがって、上記キータイプ情報の第1ビット目が「1」の場合には、キー変更を行なわない限りステータス情報の第8ビット目が「0」とはならず、また、「0」の場合には、キー変更を行なうか否かに関わらず、ステータス情報の第8ビット目が「0」となっている(つまり、書換え行為が暗黙的に行なわれたことと等価になる)。

【0070】上記キーEF定義情報の書込みにおいて、書込みが正常に終了しなかった場合(ST114)、データ書込み異常を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST115)。また、書込みが正常に終了した場合(ST114)、正常終了を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST116)。

【0071】図10は、キーデータ設定のための動作を説明するフローチャートを示しており、以下それについて説明する。ICカード1が、外部から入力されるキーデータ設定コマンドを受信すると、まず、カレントDFを認識する(ST31)。

【0072】カレントDFを認識すると、次に、コマンド電文にて指示されているエレメンタリファイル名(EF-ID)を参照し、アクセス対象となっているカレントDF内に、当該エレメンタリファイル名が存在するか否かをチェックする(ST32)。もし存在しない場合

には、該当キーID無しを意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST33)。

【0073】もし存在すれば、次に当該キーEF定義情報中のアクセス条件情報のうち、キーデータ設定に関する情報を参照する。この条件と、後述するRAM上の照合状態保持領域Aのみを比較し、アクセス条件が要求しているキーの照合状態が確立されているか否かを判断する(ST34)。

【0074】もし確立されていなければ、アクセス条件不一致を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST35)。また、もし確立されていれば、次に、対応するキーEF領域内にキーデータが存在するか否かを確認する(ST36)。もし存在すれば、既存キーデータ有りを意味するレスポンスデータを出力し、コマンド待ち状態に戻る(ST37)。

【0075】もし存在しなければ、コマンド電文にて指定されたキーのタイプと、入力キーデータのサイズの正当性をチェックする(ST38)。このとき、キーのタイプが「認証関連キー」となっていればサイズが例えば8バイト、また、キーのタイプが「照合キー」となっていればサイズは例えば1~16バイトであるとき、サイズが正当であると判断する。もし正当でないと判断された場合には、入力キーデータサイズ異常を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST39)。

【0076】ここで、サイズが正当であったと判断された場合には、次に、当該キーEF定義情報中にて定義されているサイズと、入力されたキーデータのサイズとの比較を行なう(ST40)。後者のサイズに例えば「2」を加えたものが、前者のサイズよりも大きい場合には、領域サイズ不足を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST41)。

【0077】そうでなければ、受信したコマンドにて入力されたキーデータに、1バイトの長さの情報および1バイトのBCCを付加して、これを当該キーEF領域に格納し(ST42)、処理結果をレスポンス電文にて出力し、コマンド待ち状態に戻る(ST43)。

【0078】図11は、キーデータ変更のための動作を説明するフローチャートを示しており、以下それについて説明する。ICカード1が、外部から入力されるキーデータ変更コマンドを受信すると、まず、カレントDFを認識する(ST51)。

【0079】カレントDFを認識すると、次に、コマンド電文にて指示されているエレメンタリファイル名(EF-ID)を参照し、アクセス対象となっているカレントDF内に、当該エレメンタリファイル名が存在するか否かをチェックする(ST52)。もし存在しない場合には、該当キーID無しを意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST53)。

【0080】もし存在すれば、次に当該キーEF定義情

報中のアクセス条件情報のうち、キーデータ変更に関する情報を参照する。この条件と、後述するRAM上の照合状態保持領域AおよびBを比較し、アクセス条件が要求しているキーの照合状態が確立されているか否かを判断する(ST54)。

【0081】もし確立されていなければ、アクセス条件不一致を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST55)。また、もし確立されていれば、次に、対応するキーEF領域内にキーデータが存在するか否かを確認する(ST56)。もし存在しなければ、既存キーデータ無しを意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST57)。

【0082】もし存在すれば、コマンド電文にて指定されたキーのタイプと、入力キーデータのサイズの正当性をチェックする(ST58)。このとき、キーのタイプが「認証関連キー」となっていればサイズが例えば8バイト、また、キーのタイプが「照合キー」となっていればサイズは例えば1~16バイトであるとき、サイズが正当であると判断する。もし正当でないと判断された場合には、入力キーデータサイズ異常を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST59)。

【0083】ここで、サイズが正当であったと判断された場合には、次に、当該キーEF定義情報中に定義されているサイズと、入力されたキーデータのサイズとの比較を行なう(ST60)。後者のサイズに例えば

「2」を加えたものが、前者のサイズよりも大きい場合には、領域サイズ不足を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST61)。

【0084】そうでなければ、受信したコマンドにて入力されたキーデータに、1バイトの長さの情報および1バイトのBCCを付加して、これを当該キーEF領域に格納し(ST62)、その処理結果をレスポンス電文にて出力し、コマンド待ち状態に戻る(ST63)。また、このとき、キーEF定義情報にあるステータス情報の第8ビット目を「0」とする。

【0085】図12は、キー照合のための動作を説明するフローチャートを示しており、以下それについて説明する。ICカード1が、外部から入力されるキー照合コマンドを受信すると、まず、カレントDFを認識する(ST71)。

【0086】カレントDFを認識すると、次に、ディレクトリ121を検索することにより、カレントDF内に指定されたファイル名(ID)を有するキーEF定義情報が存在するか否かを確認する(ST72)。もし存在しない場合には、該当キーID無しを示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST73)。

【0087】もし存在していた場合には、当該キーがロック状態になっているか否かを確認する(ST74)。このとき、ロック状態であると判断した場合には、キーロックを示すレスポンス電文を出力し、コマンド待ち状

態に戻る(ST75)。

【0088】もしそうでなければ、コマンド電文内のキーデータと、当該キーEF内に格納されているキーデータとを照合する(ST76)。このとき、両者が一致している場合には(ST77)、当該キーEF定義情報中の照合ビット指定情報を参照し、所定のRAM領域の当該情報にて指定されているビット位置を「1」にする(ST78)。次に、当該キーEF定義情報中のキー固有の照合不一致カウンタをクリアし(ST79)、正常終了を示すレスポンス電文を出力して、コマンド待ち状態に戻る(ST80)。

【0089】なお、所定のRAM領域は、照合状態保持領域AおよびBに分割されている。どちらの領域の対応ビットを「1」にするかは、当該キーEF定義情報中のキーのステータス情報の第8ビット目の値に依存する。このビットは、当該キーEF定義情報により定義づけられているキーに対し、変更処理が行なわれたか否かを示すものであり、後述するように、「0」となっていれば変更されたキーであり、「1」となっていれば変更処理が行なわれていないキーであることを示す。さらに、これが「0」となっていた場合には、前記照合状態保持領域Aの、また、「1」となっていれば、前記照合状態保持領域Bの、対応ビットを設定することになる。

【0090】また、キー照合処理において、不一致であると判断した場合には(ST77)、まず、当該キーEF定義情報中の照合ビット指定情報、および、ステータス情報を参照し、上記と同様の手順にしたがって、照合状態保持領域AまたはBのいずれかの領域の所定ビットを「0」にする(ST81)。

【0091】次に、キー固有の照合不一致カウンタを1つだけインクリメントする(ST82)。このとき、キーEF定義情報中のカウンタ最大値に達していない場合には(ST83)、照合不一致を示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST84)。また、最大値に達していたならば、キーロック済みを示すレスポンス電文を出力し、コマンド待ち状態に戻る(ST85)。

【0092】照合状態保持領域Aは、ファイル創成時、キーEF創成時、キーデータ創成時、キーデータ変更時に参照され、照合状態保持領域Bはキーデータ変更時に参照される。

【0093】上述したように、キーが変更済みの場合照合状態保持領域Aが、未変更であれば照合状態保持領域Bのビットがオンされるので、ファイル創成時、キーEF創成時、キーデータ創成時にはキーが変更済みでなければならない。又、キーの変更時には照合状態保持領域A及びBを参照するのでキーが変更済みであっても未変更であってもキーの変更は可能となる。

【0094】図13は、データEFへのアクセスのための動作を説明するフローチャートを示しており、以下そ

10

20

30

40

50

れについて説明する。ICカード1が、外部から入力されるデータEFアクセスコマンドを受信すると、まず、カレントDFを認識する(ST91)。

【0095】カレントDFを認識すると、次に、コマンド電文にて指示されているエレメンタリファイル名(EF-ID)を参照し、アクセス対象となっているカレントDF内に、当該エレメンタリファイル名が存在するかどうかをチェックする(ST92)。もし存在しない場合には、該当キーID無しを意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST93)。

【0096】もし存在すれば、次に当該データEF定義情報中のアクセス条件情報のうち、アクセスのタイプ(データ読出し/書込み/変更)に対応するアクセス条件情報を参照する。この条件と、後述するRAM上の照合状態保持領域Aを比較し、アクセス条件が要求しているキーの照合状態が確立されているかどうかを判断する(ST94)。

【0097】もし確立されていなければ、アクセス条件不一致を意味するレスポンス電文を出力し、コマンド待ち状態に戻る(ST95)。もし確立されていれば、次に、対応するデータEF領域内に対してアクセスを行ない(ST96)、その処理結果をレスポンス電文として出力し、コマンド待ち状態に戻る(ST97)。

【0098】次に、このような構成において、ICカードに対して各ファイルを創成する手順を説明する。

【0099】まず、ICカードを製造する際に、カード発行者に渡すべきトランスポートキーのエレメンタリファイルを設定(創生)するために、図9のフローチャートに従って図14に示すようにマスタファイル(MF)配下に“キーEF-a”を創成し、ここにトランスポートキーを設定する。

【0100】続いて当該キーエレメンタリファイルEF-aへの中の設定が図10のフローチャートに従って設定され、キーの設定に際しては、当該キーEF-aに付与されているキー設定用のアクセス条件が参照される。

【0101】この状態で発行者がカードを受け取ると、図11のフローチャートに従ってトランスポートキーを変更する。すなわち図15に示すように発行者は、製造者が設定したトランスポートキーを自身のみが知りえるキー(a')に変更する。この変更には、当該キーEFに設定されているキー変更用のアクセス条件を参照する。この時点で、マスタファイル(MF)に付与されているトランスポートビットがオンされ、以降、製造者によるマスタファイル(MF)配下のキーの創成が拒絶される。

【0102】つぎに、発行者は、自身が必要とするデータEF-aをマスタファイル(MF)配下に創成する。この場合、マスタファイル(MF)に設定されているEF創成用アクセス条件を参照する。

*【0103】また発行者は、アプリケーション提供者に開放するためのデータファイル(DF)を、マスタファイル(MF)配下に創成する。DFの設定は図7のフローに従って行われ、この場合、マスタファイル(MF)に設定されているデータファイル(DF)創成用アクセス条件を参照する。

【0104】つぎに、発行者は当該データファイル(DF)配下に、アプリケーション提供者に渡すべきトランスポートキーEF-bを創成する。トランスポートキーEF-bの創成は図9のフローに従って行われ、この場合、参照するアクセス条件は当該データファイル(DF)に付与されているものではなく、その親ファイルであるマスタファイル(MF)に付与されているアクセス条件を参照する。

【0105】つぎに発行者は、このトランスポートキーEF-b内に、トランスポートキーを設定する。トランスポートキーの設定は図10のフローに従って行われ、この場合、対象となっているキーEF-bに付与されている、キー設定用のアクセス条件を参照する。

【0106】この状態でアプリケーション提供者がカードを受け取ると、図16に示すようにアプリケーション提供者は、発行者が設定したトランスポートキーを自身のみが知りえるキー(b')に変更する。この変更には、当該キーEFに設定されているキー変更用のアクセス条件を参照する。この時点で、データファイル(DF)に付与されているトランスポートビットがオンされ、以降、発行者によるデータファイル(DF)配下のキーの創成が拒絶される。

【0107】つぎに、アプリケーション提供者は、自身が必要とするデータEF-bをデータファイル(DF)配下に創成する。データEF-bの創成は図7のフローに従って行われ、この場合、データファイル(DF)に設定されているEF創成用アクセス条件を参照する。

【0108】またアプリケーション提供者は、自身が必要とするキーEF-cをデータファイル(DF)配下に創成する。キーEF-cの創成は図8のフローに従って行われ、この場合も、データファイル(DF)に設定されているEF創成用アクセス条件を参照する。

【0109】コマンドが下記のようになり、特に、通常のキーEF創成コマンドとトランスポートキーEF創成コマンドとは別のコマンドコード形式となっていて、ICカードはこのコマンドコードによりコマンドの内容を識別している。

【0110】すなわち、通常のキーEF創成コマンドとトランスポートキーEF創成コマンドとを識別し、トランスポートキーEF創成コマンドの場合は図9のフローチャートにより処理され、通常のキーEF創成コマンドの場合は図8のフローチャートにより処理される。

*【0111】

エリア(エレメンタリファイル)創成コマンド

コマンドコードA/AID(EF-ID)/ASIZ/AAC
 キーEF創成コマンド
 コマンドコードB/KID/KSIZ/CF/AAC
 トランспортキーEF創成コマンド
 コマンドコードC/KID/KSIZ/CF/AAC

上述したカレントDF配下にトランспортキーEFを創成する場合はカレントDFの親DFのアクセス条件を参照する。親DFのアクセス条件は上位者が設定したものであり、トランспортキーEFの創成は上位者が行うことができる。

【0112】また、トランспортキーEFへのトランспортキーの設定時は当該EFのアクセス条件を参照するが、当該EFのアクセス条件はトランспортキーEFの創成時に上位者が設定するものであり、上位者はトランспортキーEFへのトランспортキーの設定が可能となるように当該EFのアクセス条件を設定する。

【0113】カレントDF配下にアプリケーション提供者がキーEFを設定する場合はカレントDFのキーEF創成用のアクセス条件が参照されるが、DFのアクセス

条件はDF創成時に上位者が設定することとなる。【0114】しかし、トランспортキーの変更後はこのDFのアクセス条件を用いる処理(データEF、キーEFの創成)はアプリケーション提供者しかおこなうことはできないので、アクセス権の区分は明確となる。

【0115】さらに、キーEF創成用のアクセス条件として上位者がトランспортキーの変更後のキーを設定しておくことでアプリケーション提供者はトランспортキーを変更した後に自身で用いるキーEFを設定し、この自身で用いるキーEFのキーの定義情報中の照合ビット指定情報によりDFのアクセス条件を満足できる環境を用意し、そして、自身のキーを照合するとデータEFの創成のためのDFのアクセス条件が満足されて、データEFの創成が可能となるようにしておく。

【0116】このようにすることで、上位者はDFのアクセス条件は設定するものの、その内容については関知することなく、アプリケーション提供者のみがDFのアクセス条件を満足できるようになる。

【0117】以上説明したように上記発明の実施の形態によれば、データファイル(DF)配下にEF(またはDF)を創成するために必要となるキーは、当該データファイル(DF)に付与されているアクセス条件により決定され、またこのアクセス条件は、上位のキー(この実施例においては、発行者が、アプリケーション提供者にとっての上位者になる)を指定することなく実現することができる。

【0118】従って、アプリケーション提供者が自身で管理したいファイル(またはメモリ領域)は、自身のみで保護することができる。

【0119】これにより、発行者の当該データファイル

(DF)への関与がなされなくなり、従って、発行者からアプリケーション提供者へ、当該ファイル(またはメモリ領域)へのアクセスの権限が委譲されたことになる。

10 【0120】なお、本実施例にあるトランспортビットは、データファイル(DF)創成時にはオフとなっており、トランспортキー自身がキー変更コマンドにより変更された時点でオンとなる旨を記載しているが、キー変更コマンドと連動することなく、例えばトランспортビットをオンするコマンドにて実施してもよい。この場合、当該コマンドを実行する際に使用されるアクセス条件は、対象とするファイルに設定されているものが参照される。

20 【0121】また、前記実施の形態では、メモリのアクセス管理を行なう電子機器としてICカードを例示したが、これに限定されることなく、メモリのアクセス管理を必要とするメモリを備えた電子機器であれば適用可能である。

【0122】

【発明の効果】以上詳述したように本発明によれば、たとえば、上位者からのデータファイルへの関与をなくし、上位者から下位者へ当該データファイルまたはメモリ領域へのアクセスの権限を委譲することができるメモリのアクセス管理方法を提供できる。

30 【図面の簡単な説明】

【図1】本発明の実施の形態に係るICカードが適用されるカード取扱装置の構成例を示すブロック図。

【図2】ICカードの構成例を示すブロック図。

【図3】データメモリの構成例を示すメモリマップ図。

【図4】各種定義情報のフォーマット例を示す図。

【図5】データメモリ内に設定されるファイルの構造例を示す図。

【図6】データメモリ内に設定されるディレクトリの構成例を示す図。

40 【図7】データファイル創成のための動作を説明するフローチャート。

【図8】キーエレメンタリファイル創成のための動作を説明するフローチャート。

【図9】トランспортキーエレメンタリファイル創成のための動作を説明するフローチャート。

【図10】キーデータ設定のための動作を説明するフローチャート。

【図11】キーデータ変更のための動作を説明するフローチャート。

50 【図12】キー照合のための動作を説明するフローチャ

ート。

【図13】データエレメンタリファイルへのアクセスのための動作を説明するフローチャート。

【図14】製造者によるICカードに対するファイル創成を説明するための図。

【図15】発行者によるICカードに対するファイル創成を説明するための図。

【図16】アプリケーション提供者によるICカードに対するファイル創成を説明するための図。

【符号の説明】

1…ICカード

2…カードリーダー・ライター

3…制御部

4…キーボード

5…CRTディスプレイ装置

11…制御素子

12…データメモリ

13…ワーキングメモリ

14…プログラムメモリ

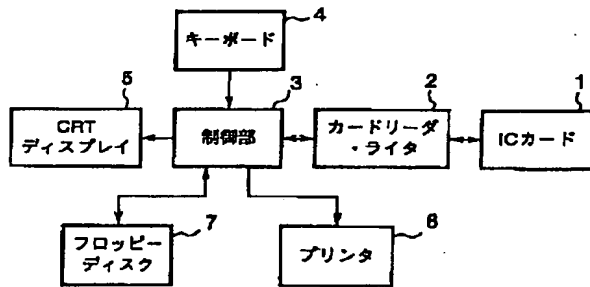
15…コンタクト部

120…制御領域

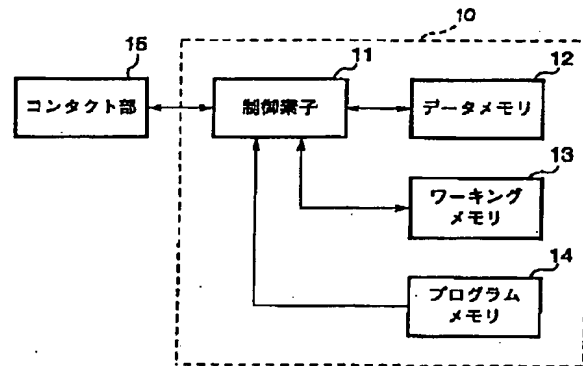
10 121…ディレクトリ

123…エリア群

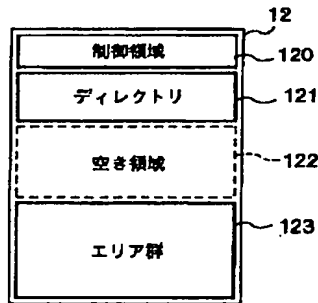
【図1】



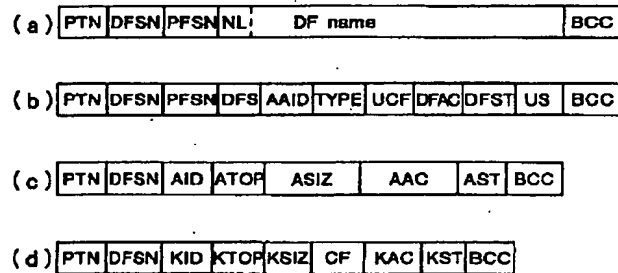
【図2】



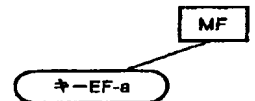
【図3】



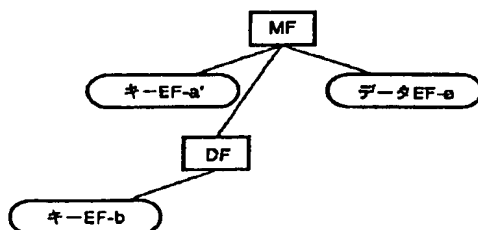
【図4】



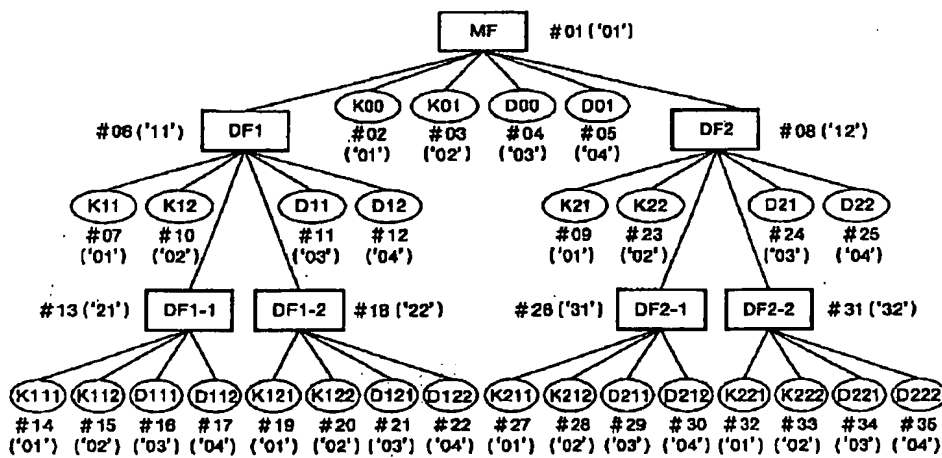
【図14】



【図15】



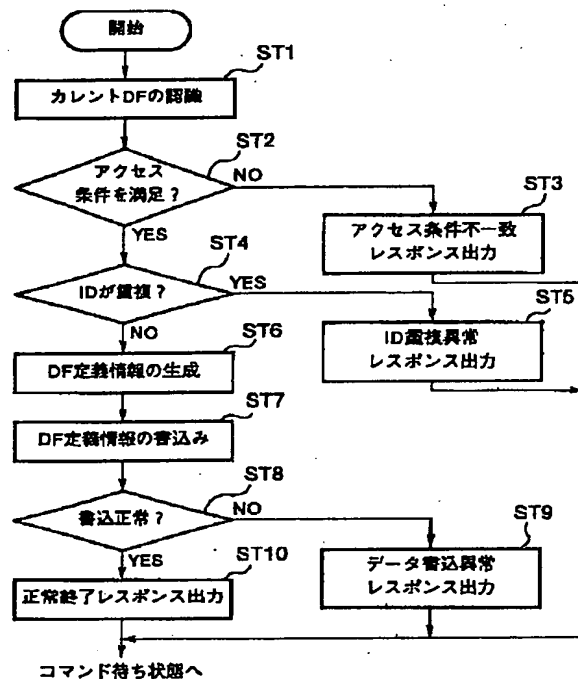
【図5】



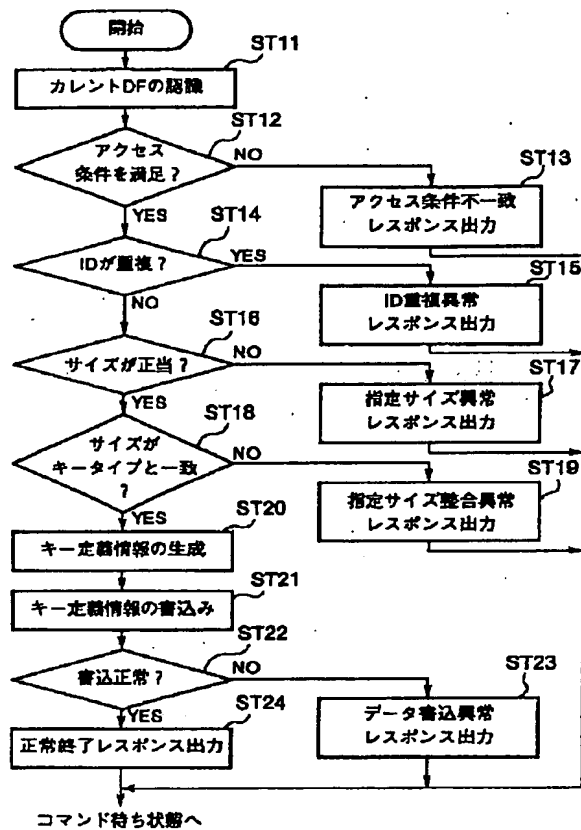
【図6】

通し番号	DFSN	PFSN	FID	
#01	00	00	00	MF 定義情報
#02	00	-	01	K00 定義情報
#03	00	-	02	K01 定義情報
#04	00	-	03	D00 定義情報
#05	00	-	04	D01 定義情報
#06	01	00	11	DF1 定義情報
#07	01	-	01	K11 定義情報
#08	02	00	12	DF2 定義情報
#09	02	-	01	K21 定義情報
#10	01	-	02	K12 定義情報
#11	01	-	03	D11 定義情報
#12	01	-	04	D12 定義情報
#13	03	01	21	DF1-1 定義情報
#14	03	-	01	K111 定義情報
#15	03	-	02	K112 定義情報
#16	03	-	03	D111 定義情報
#17	03	-	04	D112 定義情報
#18	04	01	22	DF1-2 定義情報
#19	04	-	01	K121 定義情報
#20	04	-	02	K122 定義情報
#21	04	-	03	D121 定義情報
#22	04	-	04	D122 定義情報
#23	02	-	02	K22 定義情報
#24	02	-	03	D21 定義情報
#25	02	-	04	D22 定義情報
#26	05	02	31	DF2-1 定義情報
#27	05	-	01	K211 定義情報
#28	05	-	02	K212 定義情報
#29	05	-	03	D211 定義情報
#30	05	-	04	D212 定義情報
#31	06	02	32	DF2-2 定義情報
#32	06	-	01	K221 定義情報
#33	06	-	02	K222 定義情報
#34	06	-	03	D221 定義情報
#35	06	-	04	D222 定義情報

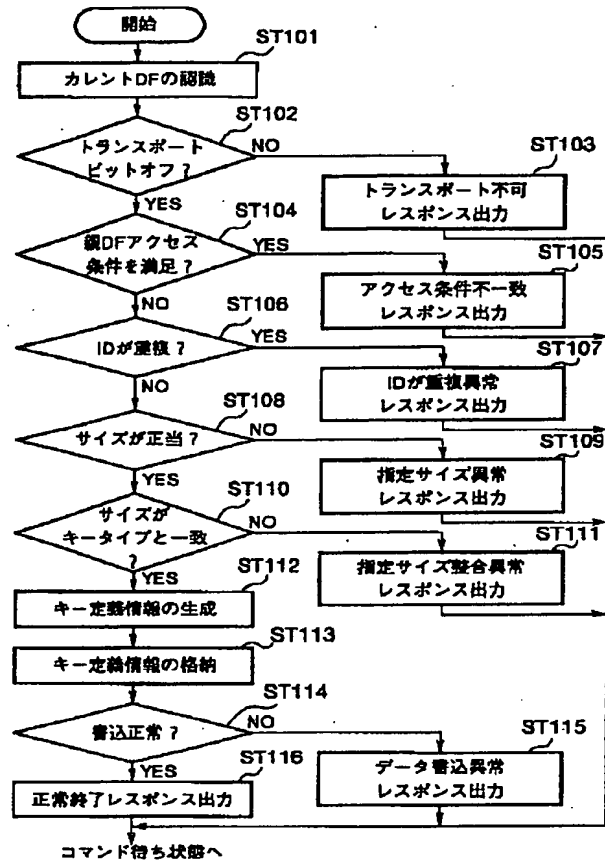
【図7】



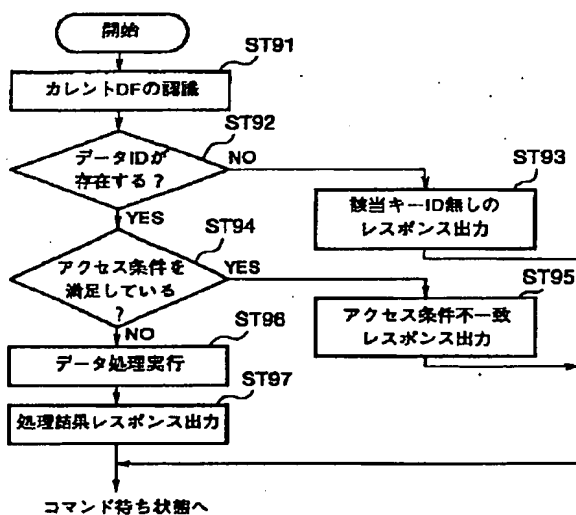
【図8】



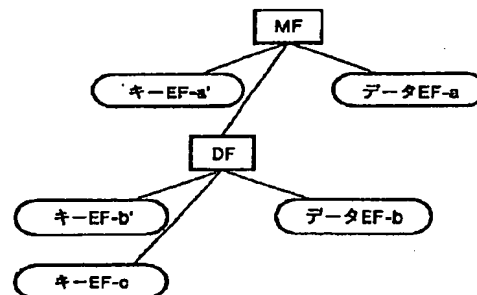
【図9】



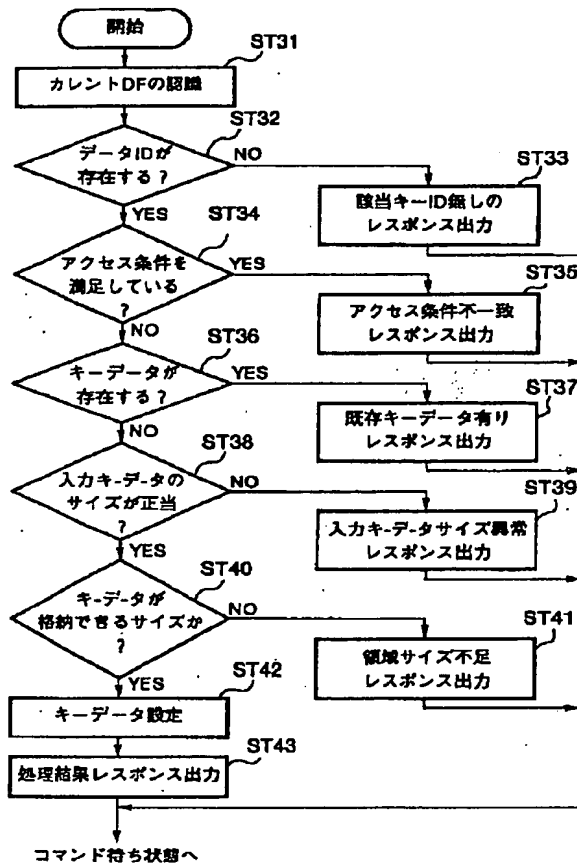
【図13】



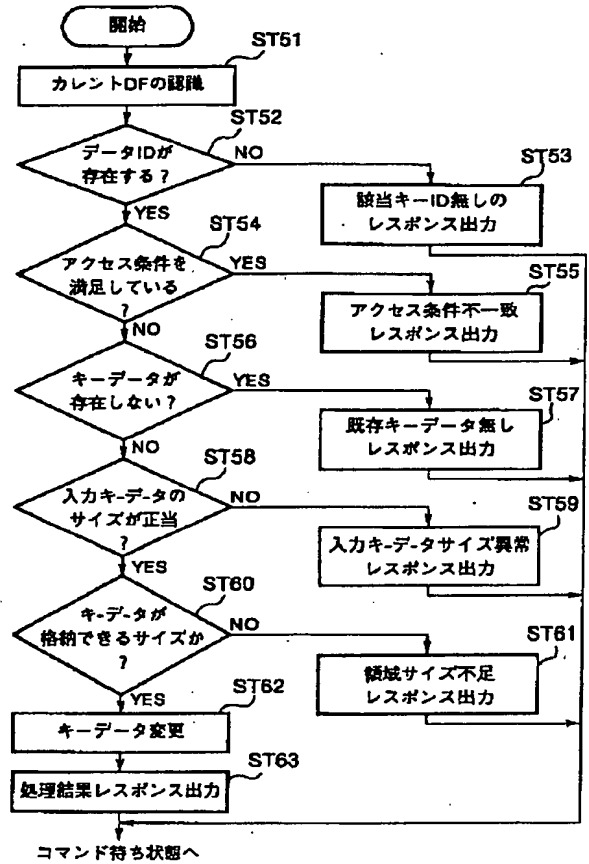
【図16】



【図10】



【図11】



【図12】

